Examples
Finite field and BCH codes

27^{th} January, 2006

1. Construct a binary BCH code of length 7 and minimum distance 3.

Solution. Here $n = 7$ and, the code being binary, q=2. Choosing r smallest such that $q^r \geq n + 1$, we have $2^r \geq 7 + 1 = 8$ and $r = 3$. Suppose $x^3 + x + 1$ is reducible, then it must have either x or $x + 1$ as a factor, and then $x = 0$ or 1 would be its root. But $x|x^3 + x + 1$ gives a remainder 1 and so does $x + 1|x^3 + x + 1$. Thus neither of these divides $x^3 + x + 1$, therefore neither is a factor of the latter, hence $x^3 + x + 1$ is irreducible.

We have $p = 2$ and $n = 3$, hence $x^{p^n-1} = x^{8-1} - 1 = x^7 - 1$.

$$\begin{array}{r|l} & x^4 + x^2 + x + 1 \\ \hline x^3 + x + 1 & x^7 - 1 \\ & x^7 + x^5 + x^4 \\ \hline & x^5 + x^4 + 1 \\ & x^5 + x^3 + x^2 \\ \hline & x^4 + x^3 + x^2 + 1 \\ & x^4 + x^2 + x \\ \hline & x^3 + x + 1 \end{array} \quad \rightarrow \quad 0 \quad \Rightarrow \quad x^3 + x + 1 | x^7 - 1$$

For $k < 7$; if $k = 6$;

$$\begin{array}{r|l} & x^3 + x + 1 \\ \hline x^3 + x + 1 & x^6 - 1 \\ & x^6 + x^4 + x^3 \\ \hline & x^4 + x^3 + 1 \\ & x^4 + x^2 + x \\ \hline & x^3 + x^2 + x + 1 \\ & x^3 + x + 1 \\ \hline & x^2 \end{array} \quad \neq 0 \quad \Rightarrow \quad x^3 + x + 1 \not| x^6 - 1$$

If $k = 5$;

$$\begin{array}{r|l} & x^2 + 1 \\ \hline x^3 + x + 1 & x^5 - 1 \\ & x^5 + x^3 + x^2 \\ \hline & x^3 + x^2 + 1 \\ & x^3 + x + 1 \\ \hline & x^2 + x \end{array} \quad \neq 0 \quad \Rightarrow x^3 + x + 1 \not| x^5 - 1$$

If $k = 4$;

$$\begin{array}{r|l} & x \\ \hline x^3 + x + 1 & x^4 - 1 \\ & x^4 + x + 1 \end{array} \quad \neq 0 \quad \Rightarrow \quad x^3 + x + 1 \not| x^4 - 1$$

When $k = 3$, $x^3 + x + 1 \not| x^3 - 1$ is obvious. Therefore $\alpha = x + \langle x^3 + x + 1 \rangle$ is a primitive. Then α satisfies $\alpha^3 + \alpha + 1 = 0$.

A minimum polynomial is a monic, irreducible polynomial of a least possible degree which has α as a root. For a finite field F or order p^n with k as its prime subfield, α and α^p have the same minimum polynomial over k for every $\alpha \in F$.

Since $p = 2$, therefore both α and α^2 have the same minimum polynomial. Then the generating polynomial is $x^3 + x + 1$. Let our message word be $a_0a_1a_2a_3$. Then the message polynomial is $a(x) = a_0 + a_1x + a_2x^2 + a_3x^3$, and the corresponding code polynomial $a(x)\left(x^3 + x + 1\right)$. Therefore the code word is

$$a_0 + (a_0 + a_1)\, x + (a_1 + a_2)\, x^2 + (a_0 + a_2 + a_3)\, x^3 + (a_1 + a_3)\, x^4 + a_2x^5 + a_3x^6$$

So our code word is

$$(a_0, (a_0 + a_1), (a_1 + a_2), (a_0 + a_2 + a_3), (a_1 + a_3), a_2, a_3)$$

Since the encoding polynomial has 3 non-zero terms, therefore the code has a minimum distance 3.
#